

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

2004年 4月28日

出願番号
Application Number:

特願2004-133100

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 2004-133100

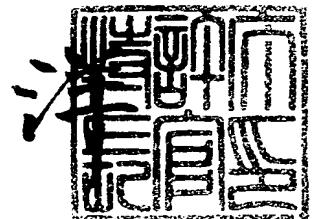
出願人
Applicant(s):

松下電器産業株式会社

2005年 6月 8日

特許庁長官
Commissioner,
Japan Patent Office

小川



BEST AVAILABLE COPY

【宣状文】
【整理番号】 2037460006
【提出日】 平成16年 4月28日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/08
【発明者】
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
【氏名】 村上 隆史
【発明者】
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
【氏名】 新谷 保之
【特許出願人】
【識別番号】 000005821
【氏名又は名称】 松下電器産業株式会社
【代理人】
【識別番号】 100097445
【弁理士】
【氏名又は名称】 岩橋 文雄
【選任した代理人】
【識別番号】 100103355
【弁理士】
【氏名又は名称】 坂口 智康
【選任した代理人】
【識別番号】 100109667
【弁理士】
【氏名又は名称】 内藤 浩樹
【手数料の表示】
【予納台帳番号】 011305
【納付金額】 16,000円
【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9809938

【請求項 1】

通信媒体から受信データを受信または通信媒体へ送信データを送信する通信媒体処理手段と、

共通鍵を配信した一般通信装置のアドレスを含む一般通信装置情報と、前記一般通信装置へ配信した共通鍵の履歴を管理する配信共通鍵保持手段と、

データ送信時に最新の共通鍵、もしくはデータ送信先の一般通信装置が保持している共通鍵を前記配信共通鍵保持手段から受け取り、データを暗号化した暗号化データを通信媒体処理手段へ渡すデータ送信処理手段と、

データ受信時にデータ送信元の一般通信装置が保持している共通鍵を前記配信共通鍵保持手段から受け取り、前記共通鍵で受信データを復号化するデータ受信処理手段と、

共通鍵を生成し、システム内に前記共通鍵を配信することによって、共通鍵を更新することを要求する共通鍵更新手段とを備えたことを特徴とする共通鍵制御装置。

【請求項 2】

前記共通鍵更新手段は、共通鍵の更新を設定した場合に、新しい共通鍵をランダム変数に基づき生成し、前記配信共通鍵保持手段で管理している前記一般通信装置が保持する共通鍵を更新することを特徴とする請求項 1 に記載の共通鍵制御装置。

【請求項 3】

前記共通鍵更新手段は、前記データ送信処理手段が送信データを暗号化する際に前記配信共通鍵保持手段から受け取った共通鍵を使用する回数がある一定回数越えた場合、もしくは前記データ受信処理手段が受信データを復号化する際に前記配信共通鍵保持手段から受け取った共通鍵を使用する回数がある一定回数を越えた場合、もしくは前記データ送信処理手段が送信データを暗号化する際に前記配信共通鍵保持手段から受け取った共通鍵を使用する回数と前記データ受信処理手段が受信データを復号化する際に前記配信共通鍵保持手段から受け取った共通鍵を使用する回数との和がある一定回数越えた場合、新しい共通鍵を生成し、前記配信共通鍵保持手段で管理しているすべての前記一般通信装置が保持する共通鍵を更新することを特徴とする請求項 1 又は請求項 2 に記載の共通鍵制御装置。

【請求項 4】

前記共通鍵更新手段は、前回共通鍵を更新してからある一定時間が経過した場合、新しい共通鍵を生成し、前記配信共通鍵管理保持手段で管理しているすべての前記一般通信装置が保持する共通鍵を更新することを特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載の共通鍵制御装置。

【請求項 5】

前記共通鍵更新手段は、前記データ受信処理手段が受信したデータの送信元の一般通信装置情報を前記配信共通鍵保持手段が保持しない場合、新しい共通鍵を生成し、前記配信共通鍵保持手段で管理しているすべての前記一般通信装置が保持する共通鍵を更新することを特徴とする請求項 1 から請求項 4 のいずれか 1 項記載の共通鍵制御装置。

【請求項 6】

前記共通鍵制御装置の前記配信共通鍵保持手段は、ネットワーク上の前記一般通信装置へ配信した共通鍵の履歴を保持し、前記共通鍵ごとに配信した前記一般通信装置のアドレスを含む一般通信装置情報を管理する共通鍵管理テーブルを保持し、前記共通鍵ごとに前記一般通信装置情報を保持することによって、前記共通鍵制御装置は前記共通鍵を配信したことがある前記一般通信装置と前記共通鍵を用いて、常に暗号化したデータを送受信することが可能にすることと、前記共通鍵を管理するための前記共通鍵管理テーブルのリソースを削減することを特徴とする請求項 1 から請求項 4 のいずれか 1 項に記載の共通鍵制御装置。

【請求項 7】

共通鍵を配信する際、前記共通鍵を暗号化するための初期共通鍵を特定の手段を用いて入力する機能を持つ初期共通鍵入力手段を保持することを特徴とする請求項 1 から請求項 6 のいずれか 1 項に記載の共通鍵制御装置。

前記初期共通鍵入力手段は、キーボード、タッチパネル、マウスといった入力装置を使用して前記初期共通鍵を入力することを特徴とする請求項7に記載の共通鍵制御装置。

【請求項9】

前記初期共通鍵入力手段は、前記共通鍵の配信先である一般通信装置のリモコンの信号を受け取る受光部であり、リモコンを使用して前記初期共通鍵を入力することを特徴とする請求項7に記載の共通鍵制御装置。

【請求項10】

前記初期共通鍵入力手段は、一般通信装置本体へ記されており、一般通信装置を梱包する袋や箱に記されておりする符号を読み取る装置であり、前記一般通信装置の符号を読み取ることで前記初期共通鍵を入力することを特徴とする請求項7に記載の共通鍵制御装置。

【請求項11】

前記初期共通鍵入力手段は、記憶媒体をインストールすることができる装置であり、前記記憶媒体をインストールすることによって前記初期共通鍵を入力することを特徴とする請求項7に記載の共通鍵制御装置。

【請求項12】

通信媒体からデータを受信又は通信媒体へデータを送信する通信媒体処理手段と、

共通鍵制御装置から配信された共通鍵と、前記共通鍵制御装置が管理するすべての前記一般通信装置が保持する共通鍵を更新している時の配信状態を示す共通鍵配信状態とを保持する共通鍵保持手段と、

データ送信時に前記共通鍵保持手段から前記共通鍵配信状態に適した共通鍵を受け取り、データを暗号化した暗号化データを通信媒体処理手段へ渡すデータ送信処理手段と、

データ受信時に前記共通鍵保持手段から前記共通鍵配信状態に適した共通鍵を受け取り、前記共通鍵で受信データを復号化するデータ受信処理手段と、

前記共通鍵制御装置へ最新の共通鍵の配信要求用データを作成し、前記データ送信処理手段へ渡す共通鍵要求手段とを備えたことを特徴とする一般通信装置。

【請求項13】

前記共通鍵要求手段は、最新の共通鍵の更新漏れを回避するために、通信できない状態であった前記一般通信装置がシステム内へ再参入する際、最新共通鍵の配信要求用のデータを作成することを特徴とする請求項12に記載の一般通信装置。

【請求項14】

前記一般通信装置の前記共通鍵保持手段が保持する前記共通鍵配信状態は、前記一般通信装置は共通鍵を配信されていないことを示す未設定状態、または、前記一般通信装置が前記共通鍵制御装置から共通鍵の更新要求を受信したことを示す配信完了状態、または、共通鍵を前記一般通信装置へ更新中であることを示す移行中状態、または、すべての一般通信装置が共通鍵の更新を完了したことを示す更新完了状態といった状態を保持することを特徴とする請求項12または請求項13に記載の一般通信装置。

【請求項15】

前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が配信完了状態である場合、前記一般通信装置は送信データを暗号化する場合、前記前共通鍵を使用して前記送信データを暗号化して送信することを特徴とする請求項12から請求項14のいずれか1項に記載の一般通信装置。

【請求項16】

前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が配信完了状態である場合、前記一般通信装置は受信データを復号化する場合、前記前共通鍵と前記新共通鍵とを使用して前記受信データを復号化し、前記前共通鍵と前記新共通鍵のどちらの共通鍵で前記受信データを暗号化されたかを特定し、前記受信データで指定する処理を行うことを特徴とする請求項12から請求項14のいずれか1項に記載の一般通信装置。

【請求項17】

前記一般通信装置は前記新共通鍵を使用して前記送信データを暗号化して送信することを特徴とする請求項12から請求項14のいずれか1項に記載の一般通信装置。

【請求項18】

前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が移行中状態である場合、前記一般通信装置は受信データを復号化する場合、前記前共通鍵と前記新共通鍵とを使用して前記受信データを復号化し、前記前共通鍵と前記新共通鍵のどちらの共通鍵で前記受信データを暗号化されたかを特定し、前記受信データで指定する処理を行うことを特徴とする請求項12から請求項14のいずれか1項に記載の一般通信装置。

【請求項19】

前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が更新完了状態である場合、前記一般通信装置は送信データを暗号化する場合、前記新共通鍵を使用して前記送信データを暗号化して送信することを特徴とする請求項12から請求項14のいずれか1項に記載の一般通信装置。

【請求項20】

前記一般通信装置の共通鍵保持手段が保持する前記共通鍵配信状態が更新完了状態である場合、前記一般通信装置は受信データを復号化する場合、前記新共通鍵を使用して前記受信データを復号化し、前記受信データで指定する処理を行うことを特徴とする請求項12から請求項14のいずれか1項に記載の一般通信装置。

【技術分野】

【0001】

ネットワークへ接続する機器へ新規に共通鍵を更新する場合、すでに配信している共通鍵を用いて、1台ずつ新規の共通鍵を暗号化して更新する場合、時間差が生じ、新規の共通鍵を保持している機器と保持していない機器がネットワーク内に存在することになる。そのような場合においても、常にネットワークに接続している機器同士で通信可能とするように制御する通信制御装置に関するものである。

【背景技術】

【0002】

従来の通信制御装置では、共通鍵を管理する通信制御装置は共通鍵を配信するだけで、その他のすべてのネットワークに接続している機器がネットワーク上に配信した共通鍵の履歴を保持するものとしていた（例えば、特許文献1参照）。すべての機器が配信された共通鍵を保持している。例えば、送信元の機器は送信データを暗号化した共通鍵を特定するために送信データの非暗号化部に共通鍵番号を付与して、送信先の機器へデータを送信する。そして、データを受信した送信先の機器は、受信データに付与している共通鍵番号から受信データを復号化するための共通鍵を選択し、受信データを復号する。このような方法によって、送信元でデータを暗号化する共通鍵と送信先でデータを復号化する共通鍵を同じものを使用した通信を実現することが可能としていた。

【特許文献1】特開2003-101533号公報

【発明の開示】

【発明が解決しようとする課題】

【0003】

しかしながら、前記従来の構成では、共通鍵の履歴をすべての機器が保持する必要があり、リソースの小さい白物家電、センサ類といったネットワークに接続する機器では配信されたすべての共通鍵の履歴を保持することは難しいという課題を有していた。

【0004】

さらに、リソースが小さく、共通鍵の履歴管理を行うことができないという理由で、配信された共通鍵を一つしか持たないような機器でネットワークを構成した場合、新たな課題が発生する。新たな課題とは、ネットワークに接続する機器が複数存在している場合、すべての機器に対して共通鍵を更新すると、共通鍵を更新する順番によって、更新後の共通鍵を保持している機器と更新前の共通鍵を保持する機器が同時に存在する場合が発生する。その時、共通鍵を更新済みの機器と、共通鍵を未更新の機器とで暗号化したデータを用いて通信を行うことができない。

【課題を解決するための手段】

【0005】

前記、従来の課題を解決するために、本発明の通信制御装置では、共通鍵を配信する装置は共通鍵更新状態管理手段と配信共通鍵保持手段を有して、共通鍵を配信される機器の負担を軽減するために共通鍵の管理を行う。

【0006】

負担を軽減化された共通鍵を配信される機器側は、共通鍵の更新状態を保持し、その状態によって保持する共通鍵の種類、データの暗号化、復号化に使用する共通鍵の選択を行う。ただし、保持する共通鍵は最大でも更新後の共通鍵および更新前の共通鍵の二種類を保持する。従来の課題を解決するために、更新後の共通鍵と更新前の共通鍵を共通鍵の更新状態によって使い分ける。従って、更新後の共通鍵を保持する機器と更新前の共通鍵を保持する機器間の通信においても、データを暗号化して通信を行うことを可能とする。

【発明の効果】

【0007】

特にホームネットワークを考慮した場合、通信システムは1：1や1：Nではなく、M

・IVによつて傳遞される。IV・IVソ連伝シヘノムシの物口、六連続で記述される機器同士の通信が行われる。共通鍵を更新している間では、更新後の共通鍵を保持する機器と更新前の共通鍵を保持する機器の間で通信が発生する可能性があるが、そのような場合においても、データを暗号化して通信を行うことができる。つまり、リソースが小さく共通鍵を配信される機器は、共通鍵の配信履歴を保持する必要なく、システム内の最新の共通鍵を保持する機器と保持していない機器間において通信することを可能とする。

【発明を実施するための最良の形態】

【0008】

以下本発明の実施の形態について、図面を参照しながら説明する。

【0009】

(実施の形態1)

図1は、本発明の実施の形態1における有線もしくは無線である通信媒体13に、共通鍵制御装置11と複数の一般通信装置12が接続しているシステム構成図である。共通鍵制御装置11は、通信媒体13に接続している一般通信装置12へ共通鍵を配信するとともに、一般通信装置12ごとに配信している共通鍵や、共通鍵の一般通信装置12への共通鍵配信状態や、配信した共通鍵の履歴を管理している。共通鍵とは、通信システム内的一般通信装置12及び共通鍵制御装置11が処理するデータを暗号・復号化する際に用いる同一の鍵である。共通鍵の一般通信装置12への共通鍵配信状態には、共通鍵を配信していない「未設定状態」、共通鍵の更新を受信した直後の状態を「配信完了状態」、システム全体で更新後の共通鍵を保持している一般通信装置12と、更新前の共通鍵を保持している一般通信装置12が混在している「移行中状態」、システム全体ですべての一般通信装置12が更新後の共通鍵を保持している「更新完了状態」といった状態がある。共通鍵配信状態の詳細な説明は後述する。

【0010】

図2は、有線もしくは無線である通信媒体22に接続する共通鍵制御装置11のプロトコルスタックを示した図である。通信媒体処理手段23は、通信媒体22へ送信データを送信し、受信データを通信媒体22から受信する。データ受信処理手段24は、通信媒体処理手段23から受信データを受け取ると、後述する配信共通鍵保持手段26から受信データの送信元へ配信している共通鍵を受け取り、受信データを復号化する。データ送信処理手段25は、後述する配信共通鍵保持手段26から送信データの送信先へ配信している共通鍵を受け取り、送信データを暗号化して通信媒体処理手段23へ渡す。ただし、送信先を特定しない例えはブロードキャストやマルチキャストでデータを送信する場合、後述する配信共通鍵保持手段26からシステム全体での最新の共通鍵を受け取り、送信データを暗号化して通信媒体処理手段23へ渡す。

【0011】

配信共通鍵保持手段26は、図5で示すような共通鍵を管理するためのテーブル51を保持している。このテーブル51の特長については、後述する。配信共通鍵保持手段26は更新した共通鍵の履歴を管理するとともに、一般通信装置12ごとに配信した共通鍵を保持しており、データ受信処理手段24がデータを受信する際、送信元の一般通信装置12が保持している共通鍵をデータ受信処理手段24へ渡し、データ送信処理手段25がデータを送信する際、送信先の一般通信装置12が保持している共通鍵をデータ送信処理手段25へ渡す。また、配信共通鍵保持手段26は、一般通信装置12から共通鍵の更新を要求するデータを受信すると、送信元の一般通信装置12へ最新の共通鍵を配信する。共通鍵更新手段27は、共通鍵を更新する際、新しい共通鍵を生成し、一般通信装置12へ配信する。

【0012】

新しい共通鍵を生成する方法として、例えはランダムで変数を作成することによって、共通鍵を生成するといった方法がある。共通鍵を更新するタイミングとしては、例えは以下のタイミングが存在する。システム使用者が、共通鍵制御装置の画面や本体から手動で更新を指定するタイミングで共通鍵を更新する。また、最新の共通鍵を使用して送信デー

ノで凹ウルバツメ由ノ一ノで後ケレに凹ウルバツメの一走凹ウルバツメに由レニノリノ、六連班を更新する。また、定期的に共通鍵を配信してから一定の時間が経過したタイミングで、共通鍵を更新する。また、配信共通鍵保持手段26で管理していない一般通信装置12から、管理している一般通信装置12へ配信した共通鍵を使用して暗号化されたデータを受信したタイミングで、共通鍵を更新する。

【0013】

図3は、有線もしくは無線である通信媒体32に接続する一般通信装置12のプロトコルスタックを示した図である。通信媒体処理手段33は、通信媒体32へ送信データを送信し、受信データを通信媒体32から受信する。データ受信処理手段34は、通信媒体処理手段33から受信データを受け取ると、後述する共通鍵保持手段36から自己の共通鍵配信状態に適した共通鍵を受け取り、受信データを復号化する。データ送信処理手段35は、後述する共通鍵保持手段36から自己の共通鍵配信状態に適した共通鍵を受け取り、送信データを暗号化して通信媒体処理手段33へ渡す。共通鍵保持手段36は、自己の共通鍵配信状態と共通鍵を保持し、共通鍵配信状態に適した共通鍵をデータ受信処理手段34及びデータ送信処理手段35へ渡す。電源OFFの状態などネットワークから離脱していた一般通信装置12がネットワークへ参入した際に、共通鍵の更新漏れを回避するために、共通鍵要求手段37は共通鍵制御装置11へ最新の共通鍵を配信することを要求する。

【0014】

図1に示すシステムのように、複数の一般通信装置12がシステム内に存在する場合、共通鍵制御装置11が共通鍵を更新する場合、システム内には更新前の共通鍵を保持する一般通信装置12と、更新後の共通鍵を保持する一般通信装置12が存在する。更新後の共通鍵を保持する一般通信装置12と保持していない一般通信装置12間の通信を可能とするための共通鍵更新シーケンスを図4に示す。

【0015】

更新前の共通鍵を「前共通鍵」、更新後の共通鍵を「新共通鍵」と呼ぶこととする。共通鍵制御装置11が管理している各一般通信装置12は、前共通鍵を保持しており、共通鍵配信状態は更新完了状態である。このとき、一般通信装置12はデータを送信する場合のデータの暗号化及びデータを受信した場合のデータの復号化には、前共通鍵を使用する。共通鍵制御装置11は、自分が管理しているすべての一般通信装置12に対して、前共通鍵で新共通鍵を暗号化して新共通鍵を配信する。新共通鍵を受信した一般通信装置12は、共通鍵配信状態を配信完了状態へ遷移させる。共通鍵配信状態が配信完了状態であるとき、一般通信装置12はデータを送信する場合のデータの暗号化には前共通鍵を使用し、データを受信した場合のデータの復号化には新共通鍵もしくは前共通鍵を使用し、新共通鍵もしくは前共通鍵のどちらで暗号化されたデータであるかを確認する。

【0016】

共通鍵制御装置11は、管理するすべての一般通信装置12へ新共通鍵を配信するデータを送信した後で、管理するすべての一般通信装置12の共通鍵配信状態を移行中状態に設定するためのデータを送信する。共通鍵配信状態が移行中状態であるとき、一般通信装置12はデータを送信する場合のデータの暗号化には新共通鍵を使用し、データを受信した場合のデータの復号化には新共通鍵もしくは前共通鍵を使用し、新共通鍵もしくは前共通鍵のどちらで暗号化されたデータであるかを確認する。そして、共通鍵制御装置11は、管理するすべての一般通信装置12へ新共通鍵を配信し、すべての一般通信装置の共通鍵配信状態を移行中状態に設定できることを確認した場合、通信管理装置11は、すべての一般通信装置12の共通鍵配信状態を更新完了状態に設定する。更新完了状態を設定された一般通信装置12は、データを送信する場合のデータの暗号化及びデータを受信した場合のデータの復号化には、前共通鍵を使用する。

【0017】

また、特に一般通信装置が家電機器やセンサ類である場合、共通鍵更新時にネットワークに接続していない可能性がある。その場合、共通鍵制御装置11は、一般通信装置12

六回鍵既にハートで交換元ハートには反映しない。六回鍵既にハートで用いながら交換ノケンスを実行することによって、共通鍵更新中に新共通鍵に更新された一般通信装置12と新共通鍵に更新されていない一般通信装置12がシステム内に混在している場合においても、一般通信装置12同士で共通鍵を使用した通信を可能とすることができます。また、一般通信装置12は、共通鍵配信状態が配信完了状態、移行中状態のときのみ新共通鍵と前共通鍵を保持し、更新完了状態の場合は新共通鍵を保持するだけによく、一般通信装置12がリソースの小さい家電機器やセンサ類であるとしても、対応が可能である。

【 0 0 1 8 】

図5に、共通鍵制御装置11の配信共通鍵保持手段26で保持する共通鍵管理テーブル51を示す。配信共通鍵保持手段26で保持する共通鍵を配信した機器ごとに管理するテーブルの特長を記載する。図5に示すように、共通鍵管理テーブルでは共通鍵を配信した履歴を管理しており、共通鍵を配信した一般通信装置12のネットワーク上のアドレスを合わせて記している。図5では、最新共通鍵はアドレスA、アドレスB、アドレスCの一般通信装置へ配信することができており、アドレスDの一般通信装置は最新の共通鍵の更新ができておらず一つ前の共通鍵である共通鍵履歴1を保持している。アドレスE、アドレスFの一般通信装置は、共通鍵履歴1及び最新共通鍵への更新ができるおらず共通鍵履歴2を保持している。共通鍵履歴3を保持する一般通信装置はシステム内には存在しておらず、アドレスGの一般通信装置は共通鍵履歴3以降の共通鍵の更新ができるおらず共通鍵履歴4を保持している。このように、共通鍵制御装置11は配信した共通鍵ごとに配信先の一般通信装置のアドレスを管理することによって、常に一般通信装置12が保持する共通鍵を使用して、一般通信装置12へデータを暗号化して送信することができ、また、一般通信装置12から受信したデータを復号化することが可能となる。

[0 0 1 9]

また、配信した共通鍵を管理する際、共通鍵管理テーブル 51 のように、配信した共通鍵の履歴ごとに配信先の一般通信装置のアドレスを管理する。また、配信していない共通鍵の履歴は削除することができる。そうすることによって、不揮発性のメモリに登録する場合でも、揮発性のメモリに登録する場合でも、共通鍵の履歴を管理する上で、最低限のメモリ使用量で、各一般通信装置へ配信した共通鍵を管理することが可能である。

[0 0 2 0]

図6は、図2で示した共通鍵制御装置11のプロトコルスタックに初期共通鍵入力手段68を追加した図である。初期共通鍵入力手段68は、配信共通鍵保持手段26にて管理していない一般通信装置宛てへ共通鍵を配信する際、共通鍵を暗号化するための初期共通鍵を入力する手段である。初期共通鍵は、配信先の一般通信装置が保持する共通鍵である。

[0 0 2 1]

一般通信装置に配信している共通鍵を外部の第三者から共通鍵を盗まれずに更新するために、前述したように、前共通鍵で新共通鍵を暗号化して新共通鍵を送信する。しかし、共通鍵を配信したことがない一般通信装置へ、共通鍵を配信する場合、共通鍵を暗号化するための前共通鍵が配信共通鍵保持手段にて保持していない。従って、初期共通鍵入力手段68から共通鍵を配信する一般通信装置12が保持する初期共通鍵を入力する必要がある。

【0022】

初期共通鍵入力手段68は、例えばキーボードやタッチパネルを使用して、一般通信装置が保持する初期共通鍵を手動で入力するものである。

[0023]

また、初期共通鍵入力手段68は、例えは一般通信装置が家電機器などである場合、その該当する家電機器のリモコンから信号を受信できる受光部であり、リモコンを使用して一般通信装置が保持する初期共通鍵を入力するものである。

【0024】

また、初期共通鍵入力手段6.8は、例えはバーコードリーダーであり、その該当する一

一般通信装置のハードウェアを読み取ることによって、一般通信装置が付与する初期共通鍵を入力するものである。

【0025】

また、初期共通鍵入力手段68は、例えばSDカード、フロッピー（登録商標）ディスク、CD-Rなどの通信一般装置に添付している記憶媒体を読み取ることができる装置であり、インストールされた記憶媒体から一般通信装置が保持する初期共通鍵を読出して入力するものである。

【0026】

また、図7に家の外にセンタサーバ71が存在しているシステムについて記載する。センタサーバ71は通信制御装置61や一般通信装置12といった機器の初期共通鍵を含むその機器に関するすべての情報を保持している。まず、初期共通鍵入力手段68は、共通鍵の配信先の一般通信装置12からその一般通信装置12の情報、例えばメーカコード、商品コード、製造番号、製造年月日を取得する。それらの情報の組合せ、もしくは単体の情報を家72の外にあるセンタサーバ71へインターネットを経由して渡し、その情報をもとにセンタサーバ71から該当する一般通信装置12が保持する初期共通鍵を取得して入力するものである。ただし、初期共通鍵を取得するためのセンタサーバ71と家72の間のインターネットを利用した通信網は、第三者が通信内容を傍受しても判断できないように、暗号化されていることが必要である。

【0027】

実際のホームネットワークにおける具体例を記載する。ホームネットワークの構成を図8に示す。図8に示すように、共通鍵制御装置であるコントローラ81と一般通信装置であるエアコン82、センサ83でホームネットワークを構成するものとする。例えば、センサは検知状態ありに変化した場合、エアコンへ動作開始の制御を行い、センサは検知状態なしに変化した場合、エアコンへ動作停止の制御を行うこととする。

【0028】

最初に、共通鍵制御装置であるコントローラ81が一般通信装置であるエアコン82、センサ83の順に共通鍵を更新する場合について記載する。コントローラ81が共通鍵更新のシーケンスを実行中、つまり、エアコン82の共通鍵を更新したが、センサ83の共通鍵をまだ更新していないときに、センサ83が検知状態ありに状態が変化し、更新前の共通鍵でデータを暗号化して、エアコン動作開始の制御要求を送信する。このとき、エアコン82の共通鍵配信状態は「配信完了」である。従って、エアコン82は受信したデータを更新後の共通鍵で復号し、暗号化した共通鍵と異なっていることを判断すると、更新前の共通鍵で受信データを復号化する。この結果、エアコン82はセンサ83から動作開始要求データを受けることができる。この例は、送信先のエアコン82と送信元のセンサ83の保持する共通鍵が異なる場合である。その後、コントローラ81はセンサ83に共通鍵を配信し、センサ83は共通鍵配信状態を内部的に「配信完了」に遷移させる。次に、コントローラ81は、共通鍵配信状態を「移行中」へ移行するようエアコン82、センサ83の順番に要求する。エアコン82に共通鍵配信状態を「移行中」へ移行する要求データを送信後に、センサ83の検知状態が「なし」へ変化した。このとき、センサ83の共通鍵配信状態は「配信完了」であるため、更新前の共通鍵を使用してエアコン82動作停止要求データを暗号化して送信する。

【0029】

受信したエアコン83は、共通鍵配信状態が「移行中」であるため、受信したデータを更新後の共通鍵で復号し、暗号化した共通鍵と異なっていることを判断すると、更新前の共通鍵で受信データを復号化する。この結果、エアコン82はセンサ83から動作停止要求データを受けることができる。その後、コントローラ81はセンサ83に共通鍵配信状態を「移行中」に移行するよう要求データを送信する。次に、コントローラ81は、共通鍵配信状態を「更新完了」へ移行するようエアコン82、センサ83の順番に要求する。エアコン82に共通鍵配信状態を「更新完了」へ移行する要求データを送信後に、センサ83の検知状態が「あり」へ変化した。このとき、センサ83の共通鍵配信状態は

「タリヤ」のものに、又机役の六通姓を伏用してノーノ動ト開如女小ノーノで呪ケルして送信する。受信したエアコン83は、共通鍵配信状態が「更新完了」であるため、受信したデータを更新後の共通鍵で復号する。この結果、エアコン82はセンサ83から動作開始要求データを受付けることができる。

【0030】

次に、コントローラ81がセンサ83、エアコン82の順に共通鍵を更新する場合について記載する。コントローラ81が共通鍵更新のシーケンスを実行中、つまり、センサ83の共通鍵を更新したが、エアコン82の共通鍵をまだ更新していないときに、センサ83が検知状態ありに状態が変化し、エアコン82動作開始の制御要求データを暗号化して送信する。このとき、センサ83の共通鍵配信状態は「配信完了」である。従って、センサ83は、更新後の共通鍵を保持しているか、更新前の共通鍵を使用してエアコン82動作開始の制御要求データを暗号化して送信する。

【0031】

エアコン82は受信したデータを、保持している更新前の共通鍵で受信データを復号化する。この結果、エアコン82はセンサ83から動作開始要求データを受付けることができる。この例は、送信先のエアコン82と送信元のセンサ83の保持する共通鍵が異なる場合である。その後、コントローラ81はエアコン82に共通鍵を配信し、エアコン82は共通鍵配信状態を内部的に「配信完了」へ遷移させる。

【0032】

次に、コントローラ81は、共通鍵配信状態を「移行中」へ移行するようにセンサ83、エアコン82の順番に要求する。センサ83に共通鍵配信状態を「移行中」へ移行する要求データを送信後に、センサ83の検知状態が「なし」へ変化した。このとき、センサ83の共通鍵配信状態は「移行中」であるため、更新後の共通鍵を使用してエアコン82動作停止要求データを暗号化して送信する。受信したエアコン83は、共通鍵配信状態が「配信完了」であるため、受信したデータをまず更新後の共通鍵で受信データを復号し、暗号化した共通鍵と同一であることを確認する。その場合、更新前の共通鍵で受信データを復号化する必要はない。この結果、エアコン82はセンサ83から動作停止要求データを受付けることができる。その後、コントローラ81はエアコン82に共通鍵配信状態を「移行中」に移行するように要求データを送信する。

【0033】

次に、コントローラ81は、共通鍵配信状態を「更新完了」へ移行するようにセンサ83、エアコン82の順番に要求する。センサ83に共通鍵配信状態を「更新完了」へ移行する要求データを送信後に、センサ83の検知状態が「あり」へ変化した。このとき、センサ83の共通鍵配信状態は「更新完了」であるため、更新後の共通鍵を使用してエアコン動作開始要求データを暗号化して送信する。

【0034】

受信したエアコン83は、共通鍵配信状態が「移行中」であるため、受信したデータをまず更新後の共通鍵で受信データを復号し、暗号化した共通鍵と同一であることを確認する。その場合、更新前の共通鍵で受信データを復号化する必要はない。この結果、エアコン82はセンサ83から動作開始要求データを受付けることができる。

【0035】

このような現象は、ホームネットワークのようにM:Nの通信システムにおいて、発生する可能性は十分高い。また、低速の通信媒体を使用している場合においては、共通鍵の更新には、さらに時間も要することとなるが、その場合も常に一般通信装置間において、通信を行うことが可能である。

【0036】

尚、本発明はプログラムによって実現することも可能である。

【産業上の利用可能性】

【0037】

本発明にかかる通信制御装置は、特にホームネットワークのようにM:Nの通信を行う

システムには用ひるこ、六邊形を大机らしい間に、システム内に大机これに六邊形を保持する機器と、保持しない機器との間でも通信を行うことが可能となる。また、本発明にかかる通信制御装置を使用して共通鍵を管理することによって、特にリソースの小さい家電機器などの一般通信装置に組込むことによって効果は大きくなる。

【図面の簡単な説明】

【0038】

【図1】システム構成図

【図2】共通鍵制御装置のプロトコルスタック図

【図3】一般通信装置のプロトコルスタック図

【図4】共通鍵更新時のシーケンス図

【図5】共通鍵管理テーブルの一例を示す図

【図6】共通鍵制御装置のプロトコルスタック図

【図7】センタサーバが存在する場合のシステム構成図

【図8】ホームネットワークのシステム構成図

【符号の説明】

【0039】

1 1 共通鍵制御装置

1 2 一般通信装置

1 3 通信媒体

2 2 通信媒体

2 3 通信媒体処理手段

2 4 データ受信処理手段

2 5 データ送信処理手段

2 6 配信共通鍵保持手段

2 7 共通鍵更新手段

3 2 通信媒体

3 3 通信媒体処理手段

3 4 データ受信処理手段

3 5 データ送信処理手段

3 6 共通鍵保持手段

3 7 共通鍵要求手段

5 1 共通鍵管理テーブル

6 1 共通鍵制御装置

6 8 初期共通鍵入力手段

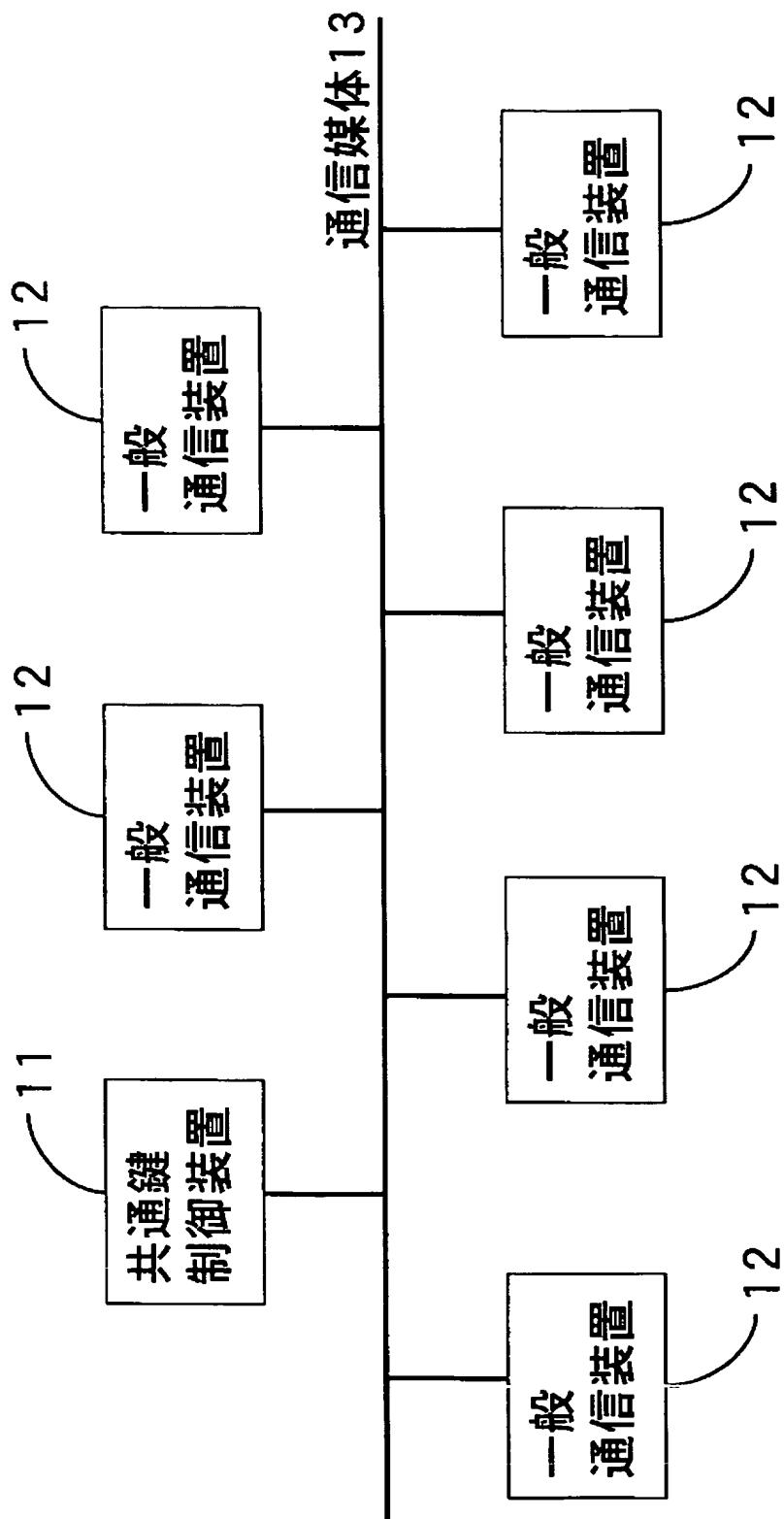
7 1 センタサーバ

7 2 家

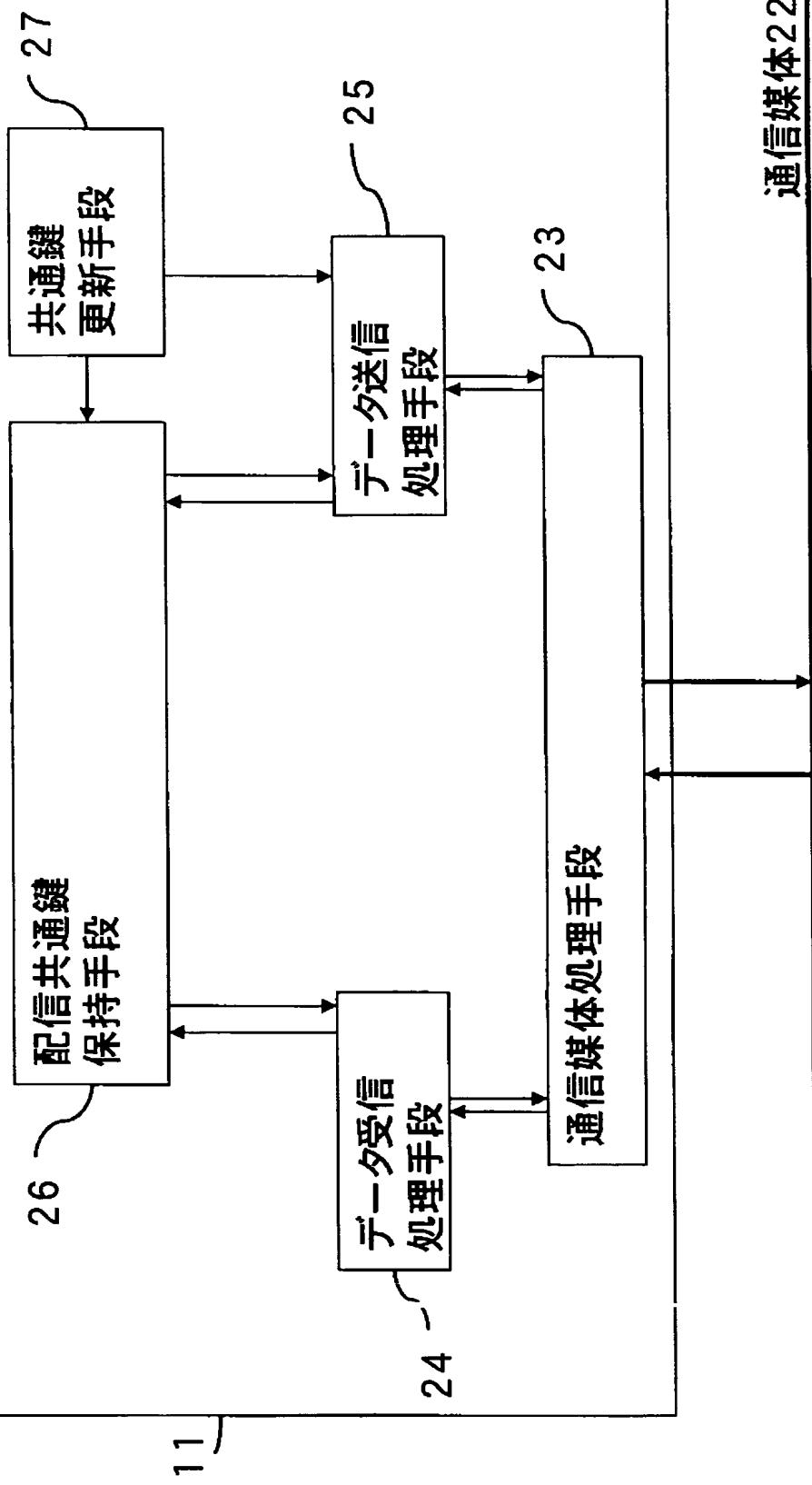
8 1 コントローラ（共通鍵制御装置）

8 2 エアコン（一般通信装置）

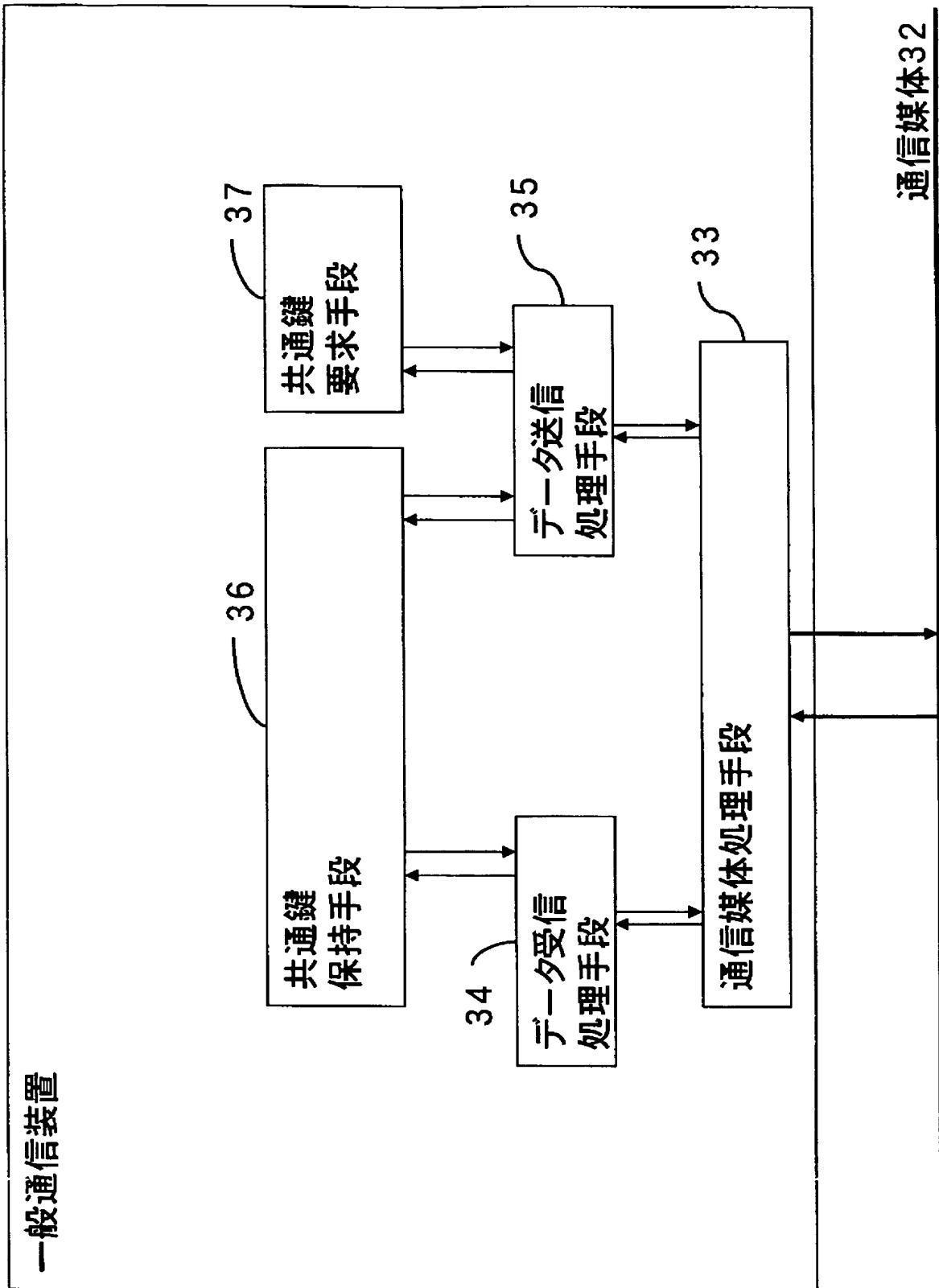
8 3 センサ（一般通信装置）

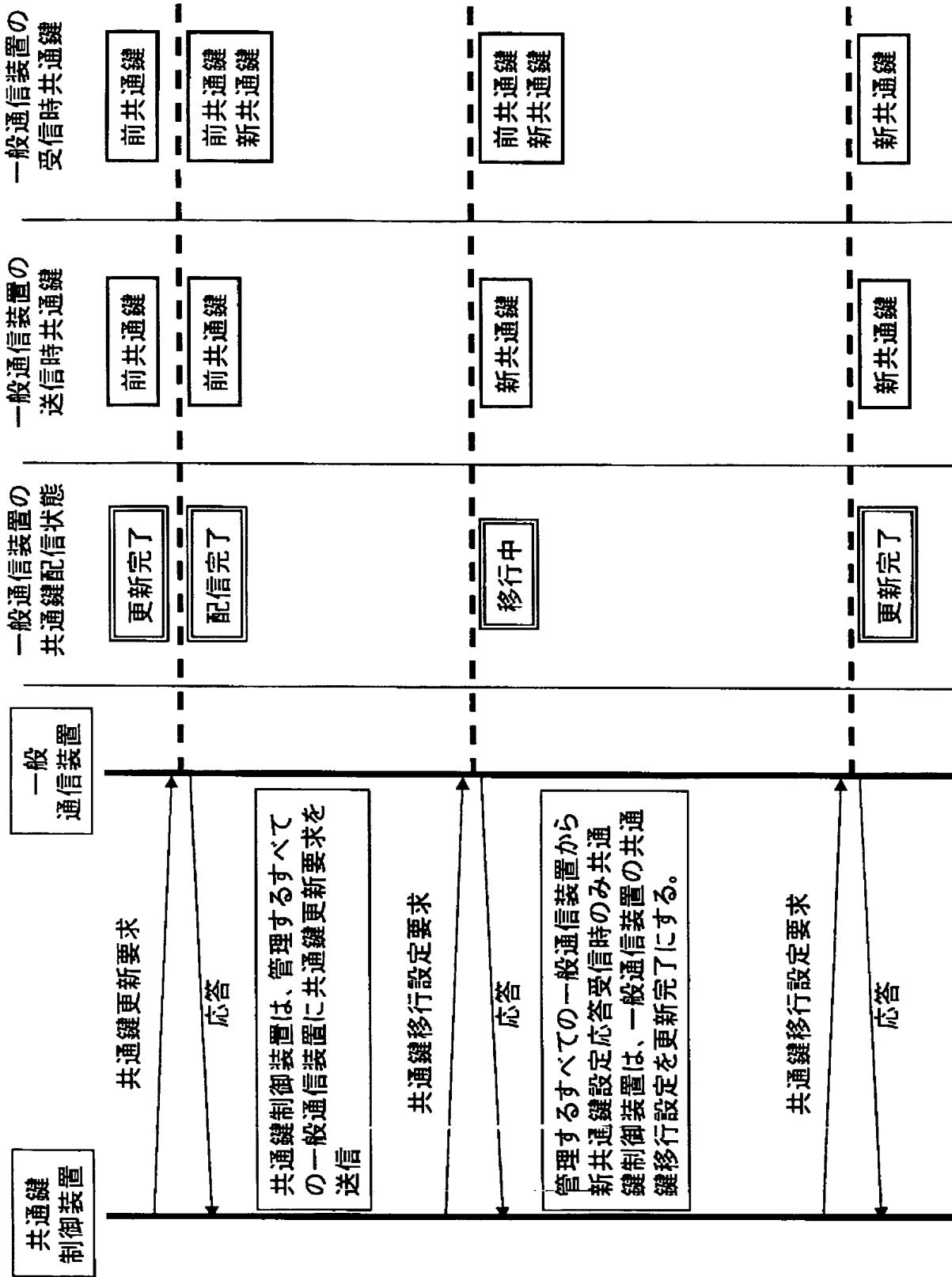


共通鍵制御装置



一般通信装置

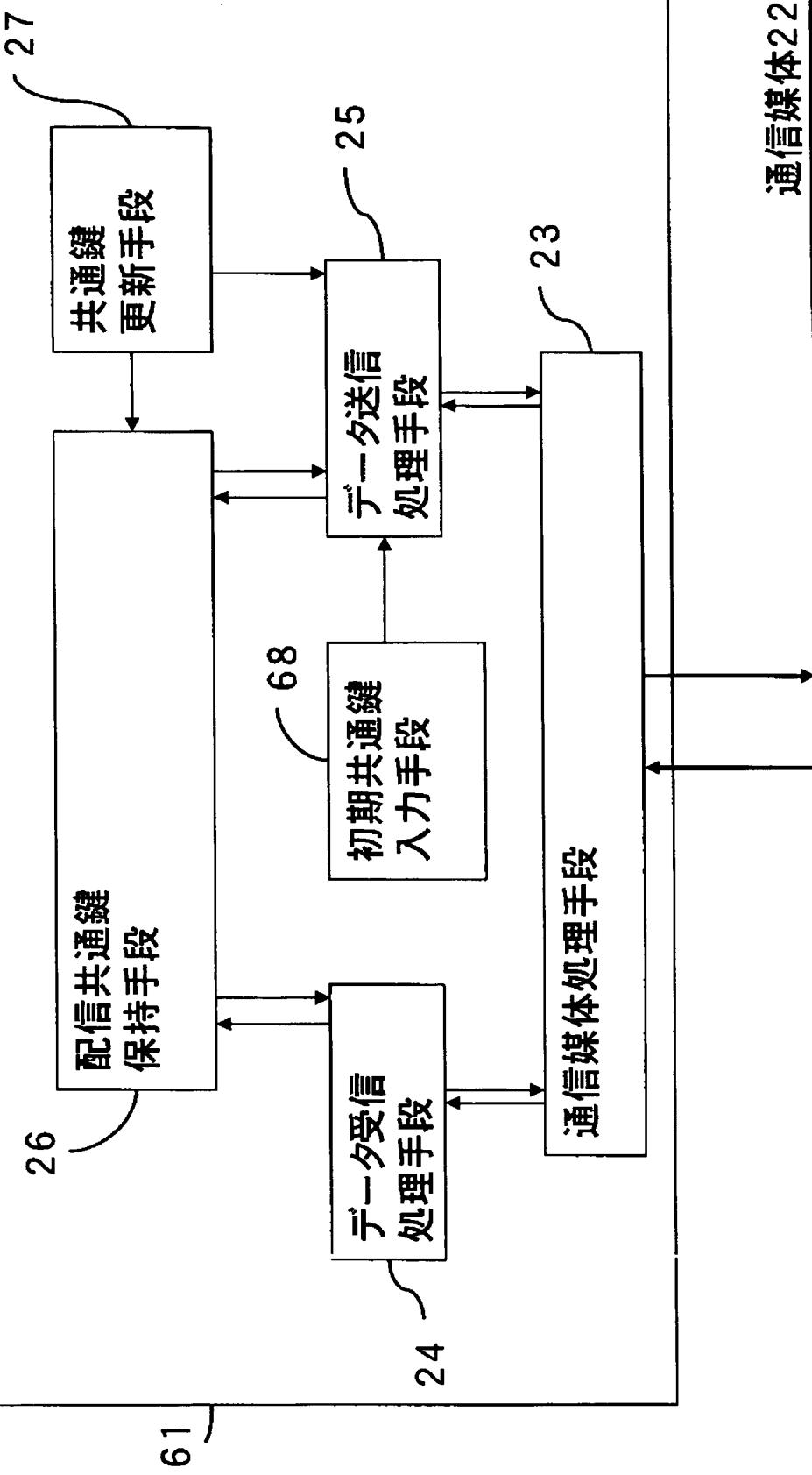


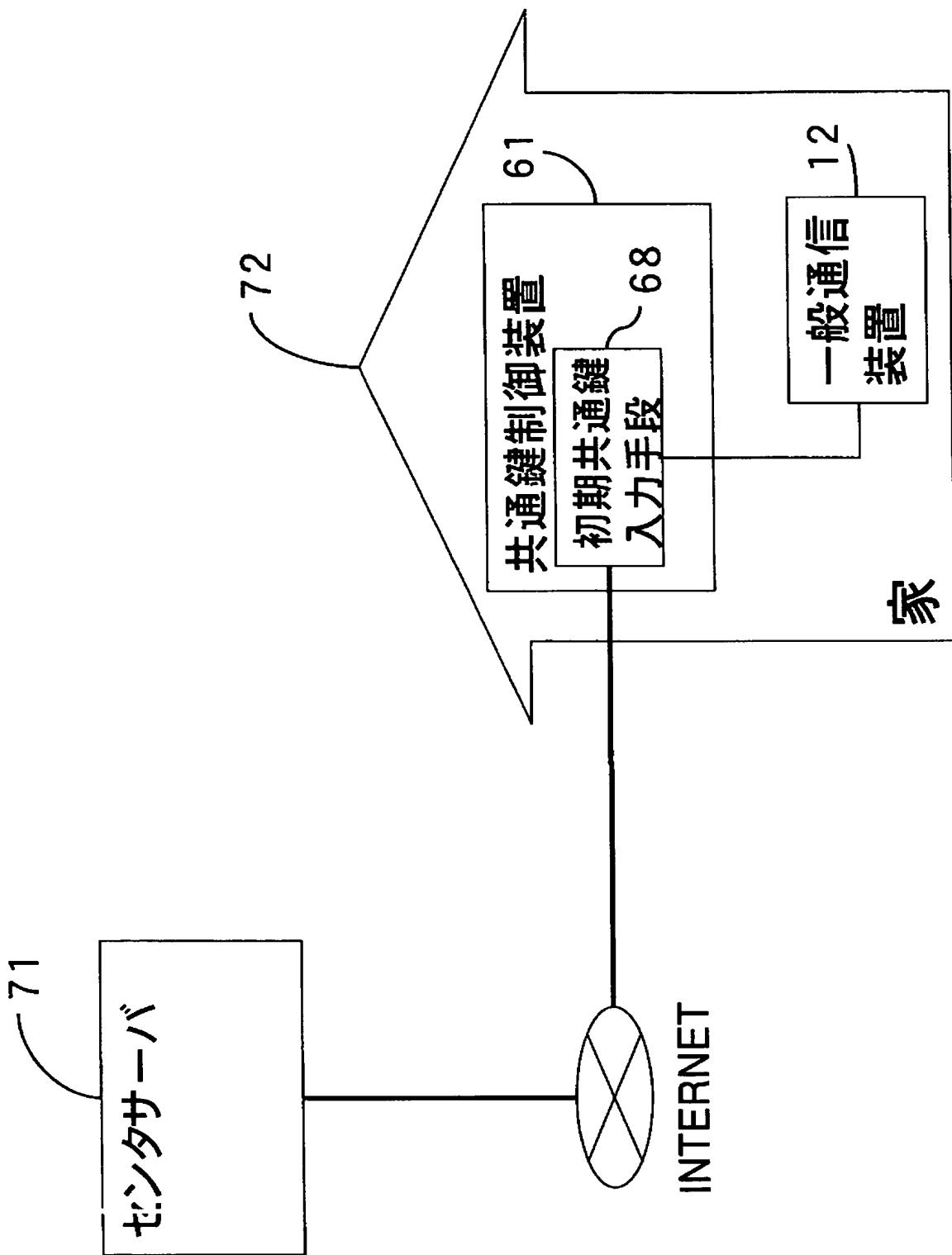


51

共通鍵	配信先アドレス
最新共通鍵	アドレスA、アドレスB、アドレスC、…
共通鍵履歴1	アドレスD
共通鍵履歴2	アドレスE、アドレスF
共通鍵履歴4	アドレスG
.	.
共通鍵履歴 n	アドレスT

共通鍵制御装置





82

エアコン
(一般通信装置)

81

コントローラ
(共通鍵制御装置)

通信媒体84

セシナ
(一般通信装置)

83

【要約】

【課題】 共通鍵制御装置がネットワークに接続している一般通信装置が保持する共通鍵を更新する際、一般通信装置が複数存在する場合、更新前の共通鍵を保持する一般通信装置と、更新後の共通鍵を保持する一般通信装置がシステム内に混在し、一般通信装置間で通信ができない状況が発生する。

【解決手段】 共通鍵を更新する中で、共通鍵配信状態を一般通信装置は保持する。一般通信装置が共通鍵を受信した際、自発的に共通鍵配信状態を変更することによって、また共通鍵制御装置が一般通信装置の共通鍵配信状態を設定することによって、一般通信装置がデータの送受信時に、更新前後のどちらの共通鍵を使用するかを決定する。その結果、更新前後の共通鍵が混在するシステムにおいても、一般通信装置間で通信を可能とする。

【選択図】 図4

000005821

19900828

新規登録

大阪府門真市大字門真1006番地

松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.